《핵심부보안방책도구》사용지도서

주체97(2008)년

1. 《핵심부보안방책도구》에 대하여

핵심부보안방책도구는 조작체계의 핵심부준위에서 위임접근조종을 실현하는데서 중요한 보안방책개발을 지원하는 도구이다.

보안방책개발도구는 보안방책에 대한 분석, 관리, 검사, 비교 기능을 가지고 있다.

1.1 보안방책분석

보안방책분석기능은 보안방책에 대한 분석을 진행할수 있다.

보안방책분석의 구체적인 기능은 다음과 같다.(표1)

표1. 보안방책분석기능

기능	설명
보안방책구성요소에 대한 검색	보안방책파일을 서술할때 구성요소의 목록을 표시한다. 례하면 령역, 형, 객체클라스, 접근벡토르, 론리형변수 등에 대한 분석을 진행한다.
보안방책규칙에 대한 검색	검색조건에 따라서 보안방책파일을 분석한다.
파일보안문맥	파일체계에 대한 파일보안문맥정보를 생성하고 그에 기초하여 파일보안문맥을 분석한다.
보안방책분석	령역이행을 나무구조로 표시하며 정보흐름을 분석한다.
보안방책파일	policy.conf파일을 표시한다.

1.2 보안방책설정

보안방책설정기능은 현재 시행되고 있는 보안방책의 기본적인 부분품들에 대한 정보를 보여주며 그에 대하여 간단한 설정을 진행할수 있게 한다.

우선 현재 시행되고 있는 보안방책의 상태를 보여준다. 즉 보안방책에 기초한 접근조종이 《시행방식》 으로 동작하는가, 《허가방식》으로 동작하는가를 보여주며 방식을 변경하는 경우에 재기동시에 파일체계에 대한 재표식을 진행할수 있도록 설정할수 있다.

다음으로 방책에 반영되여 있는 론리형값들을 통하여 기동중의 대몬들

에 대하여 유연한 접근조종을 진행할수 있다.

이 외에도 보안방책설정기능은 사용자관리와 모듈관리, 망포구에 대한 보안문맥 등 간단한 설정을 진행할수 있다.

1.3 보안방책기록검사

보안방책검사기능은 주어진 체계기록을 해석하고 모든 적재된 보안방책에 대한 통보문, AVC통보문, 론리통보문의 변경을 주어진 보안방책으로부터 추출한다.

1.4 보안방책비교

보안방책비교기능은 두개의 주어진 보안방책파일을 분석하고 그것들사이 차이점을 볼수 있게 한다.

2진 보안방책파일뿐아니라 원천 보안방책파일도 비교할수 있다.

1.5 동작환경

하드웨어환경:

중앙처리장치 : Intel Pentium IV 1.7GHz이상

물리적기억기 : 512MB 이상

하드디스크용량 : 100MB(여유용량)이상

쏘프트웨어환경:

《붉은별》사용자용체계 2.0판

2. 《핵심부보안방책도구》의 설치와 삭제

2.1 설치시 주의사항

핵심부보안방책도구를 설치하기 전에 다음과 같은 패키지들이 설치되여 있어야 한다.

selinux-policy – 보안방책패키지
checkpolicy – 보안방책콤파일러
libselinux – 파일문맥과 보안방책판정과 관련된 서고패키지
libsepol – 2진보안방책 조종과 관련된 서고패캐지
policycoreutils - 보안방책관련프로그람패키지
tcl – tcl대본작성 개발환경
tk – tcl대본작성에 기초한 도형방식의 도구묶음
매 패키지들의 판본은 해당 조작체계에 따라 다를수 있다.

이러한 패키지들이 설치되여 있지 않다면 설치전에 이 패키지들을 설치해야 한다.

2.2 설치

《핵심부보안방책도구》를 설치하는 방법은 다음과 같다.

#rpm –ivh setools-*.i386.rpm
#rpm –ivh setools-gui-*.i386.rpm
#rpm –ivh policycoreutils-*.i386.rpm

그러면 /usr/sbin/에 프로그람이 설치된다.

2.3 삭제

《핵심부보안방책도구》를 삭제하는 방법은 다음과 같다.

#r pm –e setools-gui-2.0-5.i386.rpm
#rpm –e setools-2.0-5.i386.rpm
#rpm –e policycoreutils-*.i386.rpm

3. 《핵심부보안방책도구》의 리용

3.1 기동

핵심부보안방책도구의 기동은 다음과 같다.

《시작》 -> 《체계도구》 -> 《핵심부보안방책도구》를 누르면 프로그람이 기동한다. (그림 1)

그림 1. 핵심부보안방책도구

3.2 보안방책분석

보안방책분석을 진행하려면 기본대면부에서 《보안방책분석》을 선택하고 《실행》단추를 누른다.(그림 2)
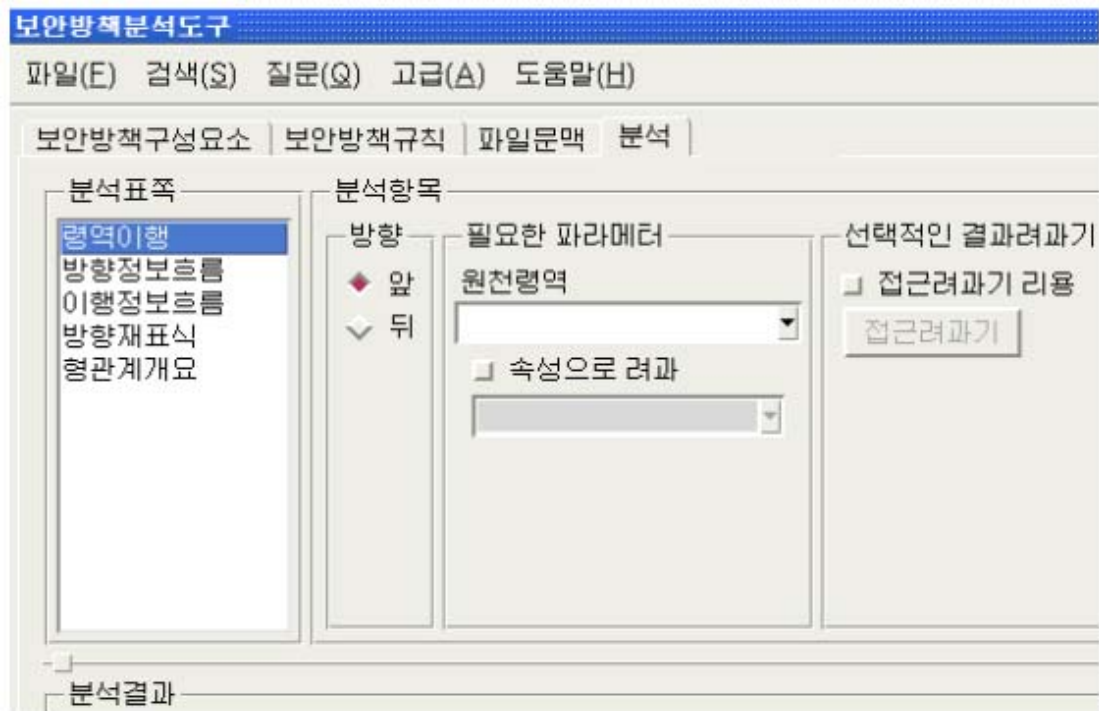
그림 2. 보안방책분석도구

보안방책분석도구는 다음과 같은 기능을 가지고 있다.

- 보안방책구성요소(형, 형속성, 객체클라스, 객체허가권한, 역할, 사용자, 론리형, 초기 보안ID, 다중준위보안, 망, 파일체계)들과 보안방책규칙(형허가, 불허가, 검사허가, 검사불허가, 형이행, 형변환)들을 검색한다.
- 파일체계에 대한 보안조작체계의 보안문맥정보를 포함하는 자료기지를 생성하고 그에 기초하여 파일의 보안문맥 혹은 보안문맥에 따르는 파일의 검색을 진행한다.
- 앞방향과 뒤방향 령역이행분석과 방향정보흐름분석, 이행정보흐름분석,방향재표식분석, 형관계분석과 같은 보안방책에 대한 분석을 진행한다.

이 도구는 또한 2진보안방책을 지원하는데 2진 또는 원천보안방책을 적재하고 보안방책분석도구의 모든 기능들을 적당하게 리용할수 있다. 일부 기능(특히 허가속성, policy.conf표시)들은 2진보안방책과 호환되지 않으

므로 그 기능들은 2진보안방책을 리용할때는 불가능하게 된다.
보안방책분석도구는 11판본부터 현재의 21판본까지의 모든 2진보안방책들에 대한 분석을 지원한다.

3.2.1 안내

파일안내는 정확히 콤파일된 원천이나 2진보안방책파일을 열수 있게 한다. 한개의 방책파일이 한번만 열릴수 있기때문에 다른 파일을 열면 현재 열려있는 파일은 닫긴다. 또한 열기선택안내항목을 리용하여 보안방책분석도구에 지정된 보안방책요소들을 적재할수 있게 된다.
검색안내는 검색결과에 대하여 행 혹은 문자렬검색을 지원한다.
질문안내는 사용자가 형시행규칙검색 혹은 분석표쪽에 렬거된 분석모듈에 대한 질문을 보관하고 적재한다. 형시행규칙질문을 보관하면 요구되는 질문파라메터의 보관도 포함하며 한편 분석질문을 보관하면 파일에 대한 전용적인 설정들은 물론 요구되는 질문파라메터들의 보관이 포함된다. 질문파일들은 '.qf' 확장자로 보관된다. 질문을 적재할때 보안방책분석도구는 지정된 질문파일을 분석할것이며 정확한 표쪽를 산생시키고 지정한 질문파라메터들과 개선된 설정들로 질문항목들을 구성할것이다. 현재 보관질문안내항목은 분석표쪽 혹은 TE규칙 표쪽(방책 규칙 표쪽 아래를 보시오)가 산생될때만 가능하게 된다. 그러나 적재질문안내항목은 모든 표쪽들에 걸쳐 가능하게 된다. 질문안내는 또한 사용자가 현재 적재된 보안방책에 대한 통계정보를 현시하도록 한다. 이 통계정보의 판본은 방책파일이 열릴때 상태띠우에 항상 현시된다.
고급안내는 분석표쪽의 방향 혹은 이행 정보흐름분석에 대하여 허가속성대응관계를 사용자가 직접 관리할수 있게 한다. 정보흐름분석을 진행하기 위해 이 대화창을 리용할 필요는 없다. 그러나 사용자는 자기가 진행하려는 주어진 분석에 대해 읽기/쓰기 접근에 대한 허가속성의 대응관계를 조종할 필요가 있게 된다. 이 대화창은 이 대응관계를 직접 조종할수 있게 한다. 기정으로 설정되여있는 대응관계는 방책으로 배포된 "mls" 파일에 기초하고 있다.

3.2.2 보안방책구성요소

이 기능은 보안방책을 구성하는 매 부분품들에 대한 검색을 진행한다.

① 형

이 기능은 형들과 속성들을 검색하게 한다. 목록안의 어떤 형이나 속성을 선택하고 마우스 오른쪽단추를 누르면 《형정보보기》, 《속성정보보기》라는 안내가 현시된다. 이것을 선택함으로써 형/속성에 대한 상세한 정보를 볼수 있다. 이것은 개별적인 형이나 속성으로 표식된 파일들을 포함하며 파일색인에 기초한 검색도 지원한다.

또한 검색항목을 선택하고 확인단추를 눌러 검색을 진행할수 있다.

② 클라스/허가권한

이 기능은 객체클라스, 공통허가권한과 방책에서 정의된 허가권한들을 보고 검색하도록 한다. 세개 목록에서 어떤 이름을 선택하고 마우스 오른쪽단추를 누르면 《객체클라스정보 표시》, 《공통허가권한클라스정보 표시》, 《허가권한정보 표시》라는 안내가 나오는데 이것을 누르면 클라스, 허가권한 혹은 공통허가권한에 대한 간단한 개요를 볼수 있다. 검색항목은 클라스들과 허가권한들에 대한 보다 구체적인 정보를 보게 한다.

실례로 객체가 허가권한 getattr을 리용하는것을 알고 싶다면 《허가권한》을 선택하고 곧바로 그 밑에 있는 《객체 클라스》단추를 누르시오. 그리고 《표현식검색》을 선택하고 "^getattr$"라고 써넣으시오. 그리고 《확인》단추를 누르고 그 허가권한을 리용하는 객체클라스들의 목록을 보시오.(a*은 클라스들이 그 허가권한을 일반적인 허가권한으로 리용한다는것을 의미한다.)

강제적인 검색을 위해 어떤 정규표현을 리용할수 있다. 그러한 실례로 문자렬 "set"로 시작되는 모든 허가속성들을 검색하기 위하여 정규표현 "^set"를 리용한다.

③ 역할

이 기능은 역할과 그것들의 속성들을 검색하게 한다. 그것은 형표쪽과 많은 측면에서 류사한다.(실례로 그 역할에 대한 상세한 설명을 보기 위해 역할을 선택하고 마우스 오른쪽단추를 누르면 《역할정보 표시》라는 안내가 나오는데 이것을 누른다.)

초보적인 검색항목으로는 주어진 형을 포함하는 모든 역할들을 검색할수 있다.

④ 사용자

이 기능은 보안방책에 정의된 사용자들을 검색할수 있으며 그 사용자에게 허가된 역할들을 검색할수 있게 한다.

⑤ 론리형

이 기능은 론리형변수의 현재 상태와 보안방책기정상태를 표시할수 있을뿐 아니라 방책에서 정의된 론리형변수를 검색할수 있게 한다. 또한 이 기능을 리용하여 론리형변수의 상태를 True나 False로 바꿀수 있다. 변경된 값은 기억기에 적재되며 실지 보안방책파일의 상태에는 영향을 주지 않는다.

⑥ 다중준위보안

이 기능은 다중준위보안을 지원하는 보안방책파일에 대하여서만 유효하다. 현재 기정으로 적재되여 있는 보안방책파일은 다중준위보안을 지원한다. 그러나 이전의 판본(판본11~판본20)들은 다중준위보안을 지원하지 않으며 따라서 이 보안방책파일들을 분석하는 경우에는 이 표쪽이 선택불가능하게 된다.

이 기능은 다중준위보안의 기본 요소인 기밀성과 분류 정보를 검색할수 있게 한다.

⑦ 초기보안ID

이 기능은 매 초기보안ID에 대한 보안문맥을 보여주며 보안방책에 정의된 초기보안ID를 검색할수 있게 한다.

⑧ 망문맥

이 기능은 망과 관련된 보안문맥들을 검색할수 있게 한다. 이 기능은 망포구, 망대면부, 말단에 대하여 검색할수 있다.

⑨ 파일체계문맥

이 기능은 파일체계과 관련된 보안문맥들을 검색할수 있게 한다.

3.2.3 방책규칙

이 기능은 보안조작체계에 대한 보다 개선된 분석을 진행하도록 한다. 이 기능들에서 사용자는 자기가 선택한 검색조건모임에 기초하여 보안방책에 있는 많은 역할들로 부터 검색하고 선택할수 있다.

① 형시행규칙

이 기능은 형시행규칙들을 검색하게 한다.(그림3)

- 규칙선택

검색령역을 결정하게 한다. 다만 선택된 규칙들은 검색에 포함된다. 만일 선택된 규칙이 없다면 검색결과가 없게 된다.

기정으로 검색조건이 다음의 보조표쪽들에서 지정되지 않았다면 보

안방책분석도구는 모든 선택된 규칙들을 검색한다.
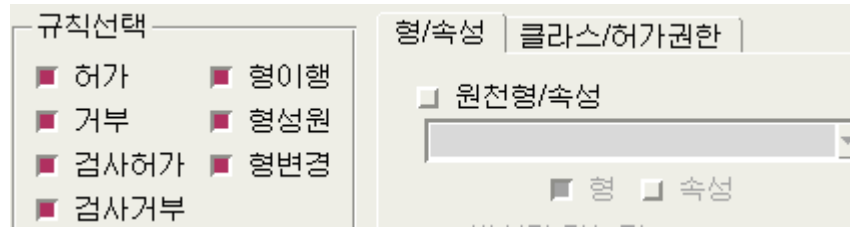
그림3. 형시행규칙

- 형/속성 보조표쪽

규칙이 리용하는 형들과 형속성들에 기초한 검색을 진행한다. 일반적으로 3개의 검색항목들이 있는데 원천형, 목적형, 기정형이 있다. 기정형은 하나 혹은 그 이상의 형이행/형성원/형변경 규칙들에 의해 유용하게 된다. 다른 규칙들은 기정형을 리용하지 않는다. 원천마당은 또한 아무 마당으로서도 리용될수 있다. 이 경우에 다른 두 항목들은 쓰지 못하게 되고 검색은 선택된 규칙들의 어떤 마당에서 선택한 형/속성을 찾게 될것이다. 내리떨구기(drop down)창은 형 혹은 속성을 선택하게 한다. 만일 《정규표현 리용》검색항목이 선택되면 형/속성 창에 표현식을 입력할수 있다. 표현식들을 사용할수 있을때 내리떨구기창을 형/속성을 선택하는데 쓴다면 형/속성문자렬은 '$' 로 둘러싸여 표현식에 따르는 정확한 정합을 진행하도록 한다.

이 문자렬은 사용자가 원하는 다른 표현식으로 편집할수 있다. 표현식이 가능하면 형과 속성 검사창들을 리용하여 형, 속성 혹은 둘다 엄밀하게 검색할수 있다. 만일 표현식이 가능하지 못하면 보안방책분석도구는 일반적으로 매 창에 오직 하나의 형/속성을 제공한다. 이 마당들에서 표현식의 리용은 다중 형/속성 선택을 가능하게 할것이다. 이 형/속성은 유효한 형 혹은 속성 문자렬이여야 한다. 기정마당은 오직 형으로만 될수 있고 속성으로는 되지 못한다.

만일 《리용가능한 규칙》검색항목이 선택되면 질문결과는 표현식에 의해 불가능으로 된 일부 규칙들을 제외하고 검색기준을 만족하는 모든 규칙들을 포함한다. 만일 이 검색항목이 선택되지 않았다면 질문결과는 표현식에 의해 불가능으로 된 일부 규칙들을 포함하며 또한 검색기준을 만족하는 모든 규칙들을 포함할것이다.

- 클라스/허가권한 보조표쪽

이 기능은 검색을 객체클라스나 허가권한을 리용하여 진행하게 한다.

다만 선택된 객체클라스들이나 선택된 허가권한들을 포함하는 규칙들만을 되돌린다. 이 개개 창들은 다중선택을 허가한다. 다중선택인 경우 보안방책분석도구는 일반적으로 《합》연산에 의하여 그것들을 취급한다.

(실례로 만일 두 객체클라스로서 등록부와 파일이 선택되였다면 파일이나 등록부객체클라스들에 적용되는 규칙들이 다 선택되게 된다.)

이 표쪽에는 또한 《허가와 검사규칙 허가권한》선택창이 있는데 이것은 선택된 객체클라스에 기초한 허가속성목록을 선택할수 있게 한다.

만일 《허가권한 려과규칙》에서 《전체(선택된 클라스)》나 《공통(선택된 클라스)》가 선택되면 선택된 객체들과 련관된 허가권한들만이 표시된다.

《형시행규칙표시》창에 주어진 검색기준을 만족하는 모든 규칙들이 현시될것이다. 만일 열려진 방책파일이 원천 policy.conf파일이라면 매 규칙에 대하여 초련결을 제공한다. 이 련결부분을 누르면 policy.conf표쪽으로 이행하며 규칙이 발견된 policy.conf파일에서 정확한 행을 강조하여 보여준다. 이것은 최종적으로 원천코드까지 규칙을 거꾸로 추적할수 있게 한다. 만일 방책이 2진방책파일이면 초련결은 제공되지 않을것이며 policy.conf 표쪽은 사용불가능하게 될것이다.

형시행규칙표쪽은 여러개의 결과들을 현시할수 있으며 만일 어떤 결과창을 선택하면 거기에 리용된 규칙 및 검색항목들을 설정할것이다.

《갱신》단추를 리용하여 현재 능동으로 선택되여 있는 결과창의 내용을 검색항목에 기초하여 변화시킬수 있다.

《새로 검색》은 현재의 검색항목들에 기초하여 새로운 결과들을 창조한다.

《형시행규칙표시》창의 아래에 있는 《닫기표쪽》띠를 사용하여 결과창문을 없앨수 있다. 또한 형시행규칙표쪽은 검색기준을 파일에 보관하고 파일로부터 규칙 및 검색항목들을 회복시키는 기능을 지원한다.

② 조건표현표쪽

이 표쪽은 검색조건표현식으로 규칙들을 현시하며 론리형값에 의한 검색을 지원한다.(그림4)

론리형값에 의한 검색에서 지원하는 보안방책규칙들은 다음과 같다.

허가, 검사허가, 검사거부, 형이행, 형성원, 형변경 규칙들이다.

그림4. 조건표현 규칙과 검색항목

검색항목으로서 론리형변수를 지정할수 있으며 정규표현을 리용한 검색도 진행할수 있다.

③ RBAC 규칙표쪽

이 표쪽은 선택된 규칙에 기초하여 RBAC규칙, 역할허가와 역할이행 규칙에 대한 검색을 지원한다.(그림5)

그림5. RBAC 규칙과 검색항목

검색항목에서 《기정역할》마당은 《규칙선택》에서 《역할이행》규칙을 선택한 경우에만 현시된다. 목적항목은 규칙이 선택되는데 따라 변화된다. 만일 허가만 선택되였다면 목표역할을 선택할수 있으며 이행만 선택되였다면 형이나 속성을 선택할수 있다.

둘다 선택되였다면 이 항목은 사용불가능하게 된다.

형시행규칙과 같이 원천항목은 아무 검색에서도 리용될수 있다.

④ 범위이행규칙표쪽

이 표쪽은 원천과 목적 형 그리고 다중준위보안에 의한 범위이행규칙(range_transition)에 대한 검색을 지원한다.(그림6)

그림6. 범위이행규칙 검색항목

범위이행규칙검색에서 3개 검색항목을 리용한다. 원천형, 목적형, MLS(다중준위보안)범위이다.

MLS범위값에 대하여 입력한 범위와 정확히 정합되는것(정합), 입력한 범위를 포함하는것(포함), 입력한 범위안에 있는 범위들을 포함(내부)하는 규칙들을 검색할수 있다.

3.2.4 파일문맥표쪽

파일문맥표쪽은 다음과 같은 기능을 제공한다.

- 색인파일을 생성과 적재

색인파일은 파일경로에 해당한 보안리눅스사용자, 형과 클라스를 포함하여 파일체계에 대한 보안리눅스문맥정보를 가지고 있는 디스크상의 자료기지이다. 이 표쪽은 색인파일을 생성하고 생성된 색인파일을 적재할수 있게 한다.

색인파일이 적재되지 않았다면 모든 검색항목은 비능동상태로 되며 색인파일이 적재되지 않았다는것을 표시한다. 《적재》단추를 누르면 적재하려고 하는 색인파일을 선택하기 위한 파일선택창이 표시된다. 《생성과 적재》단추를 누르면 색인파일을 작성하려는 목적등록부를 선택하고 색인파일 저장경로를 설정할수 있다.

- 색인파일을 검색
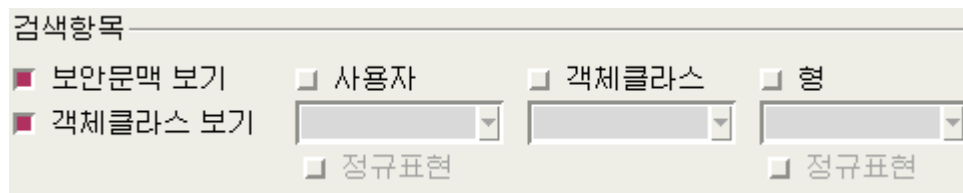
그림7. 파일문맥 검색항목

검색은 사용자, 형, 파일경로 등을 지정하여 진행할수 있다. 정규표현은 객체클라스마당을 제외한 모든 마당들에서 리용할수 있다. 《보안문맥보기》나 《객체클라스 보기》를 선택하면 검색결과에 대한 구체적인 보안문맥이나 객체클라스정보가 현시된다.(그림7)

3.2.5 분석표쪽

이 표쪽은5개의 자동화된 분석기능을 제공한다. 매 분석에서 《정보》단추는 선택된 분석기능에 대한 간단한 사용방법을 제공한다. 방책분석에 리용된 질문조건들을 《질문》안내를 리용하여 파일에 보관/적재 할수있게 한다.

① 령역이행분석

령역이행분석은 앞방향 및 뒤방향 령역이행분석을 지원한다.(그림8)

그림8. 령역이행 분석항목

- 앞방향령역이행분석

앞방향령역이행(FDT) 분석은 시작 원천령역을 가지며 시작령역으로부터 이행되는 모든 목표령역들로 이루어진 나무를 현시한다. 나무는 가능한 깊이까지 확장될수 있으며 만일 부분나무의 부모가 매듭과 같다면 더이상 확장될수 없다. 나무의 매 매듭은 목표령역을 부모령역에로 직접 이행될수 없는데까지 표시한다.

앞방향령역이행분석은 또한 명시적인 객체클라스 허가권한들에 기초하여 분석을 진행하며 개별적인 객체형(들)에 대한 접근으로 허가된 령역들에로의 이행을 검색하도록 질문을 제한할수 있게 한다. 《접근려과기》단추는 이와 같은 분석질문의 제한을 위하여 객체클라스와 허가권한, 객체형을 선택하게 한다. 기정으로 모든 객체형, 객체클라스와 허가권한은 질문에 포함된다. 목록관리창으로부터 객체클라스를 선택하면 그 객체클라스의 모든 허가권한들을 현시한다. 그러면 허가권한들은 질문에서 특정한 객체클라스 허가권한들을 포함 혹은 배제하기 위하여 라지오(radio)단추들로 현시된다.

《모든 허가권한 포함》 혹은 《모든 허가권한 제외》단추는 전체 객체클라스들을 포함 또는 제외할수 있는 기능을 지원한다.

객체클라스의 모든 허가권한들을 제외하면 질문에서 객체클라스 그 자체를 제외한다. 객체클라스가 제외되게 되면 그것이 질문에서 제외되였다는것을 표시한다.

실례를 들어 "user_t"령역으로부터 "shadow_t"령역의 파일들에 대한 쓰기접근을 가진 령역으로의 이행들을 찾는다고 하자. 이 경우에 사용자는 우선 "user_t"를 원천령역으로 지정해야 하며《접근려과기리용》을 선택하고 《령역이행접근려과기》 설정대화창에서 모든 객체클라스들을 배제하고 파일객체클라스에 대한 쓰기허가권한만을 포함시켜야 한다.

- 뒤방향령역이행분석

뒤방향령역이행분석은 앞방향령역이행분석의 반대이다. 뒤방향령역이행분석은 목적령역을 선택하며 목적령역으로 직접 이행가능힌 령역들을 나무구조로 표시한다. 나무는 가능한 깊이만큼 확장할수 있으며 만일 부분나무의 부모가 매듭과 같다면 더이상 확장될수 없다. 나무의 매 매듭은 부모매듭에로 이행할수 있는 원천령역을 표시한다. 이 분석은 접근려과를 리용할수 없다.

자식매듭을 선택하면 이행이 일어나도록 하는 모든 규칙들이 현시될것이다.

② 방향정보흐름분석

방향정보흐름분석은 시작형과 정보흐름방향(안, 밖, 안/밖, 모두)을 선택하고 뿌리매듭으로서 시작형을 설정한다.(그림9)

그림9. 방향정보흐름 분석항목

자식매듭은 정보흐름이 그의 부모매듭과 그 자체사이에서 직접 일어날수 있는 형들을 표시한다. 만일 흐름방향이 '안'이라면 자식매듭형에서 부모매듭형으로의 정보흐름을 보여준다. 만일 흐름방향이 '밖'이라면 부모매듭형에서 직접 자식매듭형으로의 정보흐름을 보여준다. 만일 방향을 '모두'로 선택하면 자식매듭에서 부모매듭으로, 부모매듭에서 자식매듭으로

의 정보흐름을 보여준다. 만일 '안/밖'이 선택되였다면 흐름방향은 '안', '밖', '모두'로 될것이다.

자식매듭을 선택하면 정보흐름이 일어나도록 하는 모든 방책규칙들이 현시될것이다. 결과는 객체클라스에 의해 표시된다.

하나이상의 객체클라스를 선택하여 결과를 려과하여 보여줄수 있다. 이것은 오직 선택된 객체클라스에서 허가된 흐름들만이 현시되게 한다. 실례로 객체클라스로 파일을 선택하면 소케트에 대해 허가된 흐름들은 현시되지 않는다.

또한 정규표현을 리용하여 끝형을 지정함으로써 현시되는 결과를 제한할수 있다. 이것은 정규표현에 맞는 끝형들만이 현시되게 한다.

③ 이행정보흐름분석

이행정보흐름분석은 보다 확장된 분석기능을 제공한다.(그림10)

그림10. 이행정보흐름 분석항목

특히 이행정보흐름분석은 두 형들사이의 간접경로를 확인할수 있게 한다.

이행정보흐름분석은 시작형과 정보흐름방향(까지 혹은 부터)을 가지고 분석을 진행하며 나무의 뿌리매듭으로 시작형을 표시한다. 자식매듭은 부모매듭과 정보흐름이 가능한 형들을 표시한다. 만일 흐름방향이 '까지'이면 부모매듭으로의 정보흐름이 일어나며 흐름방향이 '부터'이면 자식매듭으로의 정보흐름이 일어난다.

자식매듭을 선택하면 시작매듭과 자식매듭사이에 있는 흐름사슬에서 정보흐름이 일어나도록 하는 규칙에 따라서 단계별로 보여준다. 결과는 객체클라스에 의하여 표시된다.

결과본문에 시작매듭과 선택된 자식매듭사이에서 더 많은 흐름을 찾기 위하여 초련결을 제공한다. 이것은 검색에서 시간제한이나 검색에서 찾으려는 흐름수에 대한 제한을 지정할수 있게 한다.

방향정보흐름분석에서와 같이 정규표현을 리용하여 결과를 제한할수 있

다.

다음으로 이행정보흐름분석은 객체클라스 허가권한이나 형들에 의하여 결과를 려과하는 기능을 제공한다. 《이행정보흐름고급려과기》대화창에서 객체클라스를 선택하고 허가권한들을 포함하거나 제외할수 있게 함으로써 그 객체클라스에 대한 허가권한목록 선택한다. 기정으로 모든 객체클라스 허가권한들은 질문에 포함되며 그렇지 않으면 《제외》단추를 선택하여 허가권한을 제외한다. 객체클라스의 모든 허가속성들을 제외하게 되면 객체클라스 그 자체를 질문으로부터 제외하게 된다. 객체클라스가 제외되게 되면 그것이 질문에서 제외되였다는것을 표시한다.

또한 이 대화창은 적재된 허가권한대응관계에서 지적된 허가권한의 무게값을 현시한다. 허가권한을 어떤 일정한 무게값 아래보다 작은 무게를 가지는 결과로 부터 배제하기 위하여 무게턱값을 지정할수 있다. 또한 중간형을 포함 또는 제외함으로써 질문결과를 려과할수 있다.

④ 방향재표식분석

방향파일재표식분석은 객체에 허가된 형이행들과 주동체에 대해 허가된 모든 재표식허가권한에 대한 분석을 진행한다.(그림11)

그림11. 방향재표식 분석항목

이 두 방식을 각각 객체방식과 주동체방식이라고 한다.

- 객체방식

선택된 방식에 따라 서로 다른 분석결과를 현시한다. 《까지》를 선택하면 《시작형》이 재표식될수 있는 모든 형이 현시되며 《부터》를 선택하면 《끝형》이 재표식될수 있는 모든 형이 현시된다. 둘 다 선택되면 시작형/끝형이 재표식될수 있는 모든 형들이 현시된다.

- 주동체방식

이 방식에서는 주동체형을 선택하며 이 주동체형을 재표식하는 모든 형들을 두개의 목록으로 현시한다.

방향재표시분석은 정규표현을 리용하여 끌형을 지정함으로써 분석결과를 제한할수 있다. 《고급려과기 리용》을 선택하여 분석에 포함되는 객체클라스들과 재표식조작에 주동체로 포함되는 형들을 선택할수 있다.

⑤ 형관계개요분석

형관계개요분석은 두개의 형들사이의 관계를 분석할수 있게 한다.(그림 12)

그림12. 형관계개요 분석항목

방책개발자들은 형A와 형B사이에 임의의 관계(호상작용)가 존재한다면 그 관계를 빚어내는것이 무엇인가를 정확히 분석하려고 한다.

형관계개요분석은 다음의 관계들을 분석한다.

- 두 형에 공통으로 들어가는 속성(《공통속성》)
- 형A와 형B에 대한 접근권한을 가진 역할(《공통역할》)
- 형A와 형B에 대한 접근권한을 가진 사용자(《공통사용자》)
- 두 형이 공통 접근권한을 가진 객체형(《자원에 대한 류사한 접근》)
- 형A는 접근권한을 가지고 있지만 형B는 접근권한을 가지고 있지 않는 객체형(《자원에 대한 다른 접근》)
- 두 형들사이의 접근을 제공하는 규칙(형시행허가규칙)
- 두 형들사이의 이행을 허가하는 형관련규칙(형이행/형변경규칙)
- 두 형들사이의 방향정보흐름분석(A와 B사이의 방향흐름)
- 형A에서 형B에로의 이행정보흐름(이행흐름A->B)
- 형B에서 형A에로의 이행정보흐름(이행흐름B->A)
- 형A에서 형B에로의 령역이행(령역이행A->B)
- 형B에서 형A에로의 령역이행(령역이행B->A)

3.2.6 원천보안방책(POLICY.CONF)표쪽

이 표쪽은 policy.conf원천파일의 내용을 표시한다.
추가적으로 형시행규칙표쪽과 령역이행분석표쪽에서 원천보안방책파일을 열었을 때 원천policy.conf파일에로의 련결을 제공한다. 2진 보안방책파일을 분석하는 경우 이 표쪽은 사용불가능하게 되며 이 표쪽에로의 련결은 제공되지 않는다.

3.3 보안방책설정

도구는 8개의 선택항목들로 구성되여 있다.

- 상태항목

이 항목에서는 보안방책의 선택과 보안방책의 방식을 시행방식으로 하겠는가, 허가방식으로 하겠는가를 설정한다.(그림13)

체계기정시행방식 시행방식
현재 시행방식 시행방식
체계기정보안방책형 targeted
☐ 체계기동시에 재표식을 진행합니다.

그림13. 보안방책 설정

방식을 변경하는 경우 체계재기동시에 파일체계에 대한 재표식을 진행하겠는가를 문의하며 재표식을 가능하게 설정하면 다음번 체계재기동시에 파일체계 재표식을 진행한다.

- 론리형항목

이 항목에서는 일부 대몬들에 대하여 론리형변수를 리용하여 접근허가 혹은 접근거부를 설정할수 있게 한다.(그림14)

▷ CVS

▽ FTP

- ☐ 사용자홈등록부안의 파일들에 대한 읽기/쓰기권한을 ftp에 허가합니다.
- ☐ ftp봉사기가 공개파일전송봉사에 리용된 cifs를 사용하도록 허가합니다.
- ☐ ftp봉사기가 공개파일전송봉사에 리용된 nfs를 사용하도록 허가합니다.
- ☑ ftpd가 indetd가 없이도 직접 실행하도록 허가합니다.
- ☐ ftpd가 public_content_rw_t로 표식된 등록부에 파일을 올리적재하도록 허가합니다.
- ☐ ftpd대몬에 대하여 SELinux보안을 사용하지 않습니다.

그림14. 론리형항목 설정

실례로 ftp대몬에 대하여 SELinux보안을 사용하지 않게 설정하겠다 하는 경우 《ftpd대몬에 대하여 SELinux보안을 사용하지 않습니다.》라는 항목을 선택한다. 이와 같은 방법으로 요구하는 대몬에 대하여 론리형변수의 값을 반전시키는것으로 허가 혹은 거부를 설정할수 있게 한다.

론리형변수의 값은 보안방책의 판본이나 형에 따라 다를수 있다.

– 파일문맥표시

이 항목은 현재 보안방책에서 설정되여 있는 파일문맥정보들에 대한 설정을 진행할수 있게 한다.(그림15)

그림15. 파일문맥 설정

현재 설정되여 있는 파일문맥들을 보여주며 새로운 파일문맥들을 추가하고 추가한 파일문맥에 대한 변경, 삭제를 할수 있다.

새로운 파일문맥을 추가 혹은 변경하는 경우 현재 보안방책에서 정의되여 있는 형들만을 리용할수 있다. 보안방책에 정의되여 있지 않는 형을 리용하는 보안문맥을 추가할수 없다.

다중준위보안(MLS)문맥 역시 우와 같은 조건을 만족해야 한다.

- 사용자대응표항목

일반리눅스사용자와 보안리눅스(SELinux)사용자사이의 대응관계를 설정할수 있다.(그림16)

가입자 이름	SELinux 사용자	MLS/ MCS범위
__default__	user_u	s0
root	root	SystemLow-SystemHigh

그림16. 사용자대응관계 설정

사용자대응관계에 대한 추가와 변경, 삭제를 지원한다. 추가혹은 변경하는 경우 보안리눅스사용자나 다중준위보안/다중분류보안(MLS/MCS)범위가 보안방책에 정의되여 있어야 한다.

- 보안리눅스사용자항목

보안리눅스사용자는 [보안리눅스사용자]명, [표식앞붙이], [MLS/MCS준위], [MLS/MCS범위], [보안리눅스역할]에 의해 정의된다.(그림17)

SELinux 사용자	표식 앞붙이	MLS/ MCS준위	MLS/ MCS범위	SELinux역할
root	user	s0	SystemLow-SystemHigh	system_r sysadm_r user_r
system_u	user	s0	SystemLow-SystemHigh	system_r
user_u	user	s0	SystemLow-SystemHigh	system_r sysadm_r user_r

그림17. 보안리눅스사용자 설정

보안리눅스사용자 추가나 변경시 매 항목들은 보안방책에 정의되여 있는 값들을 리용하여야 한다.

- 변환항목

이 항목은 MLS/MCS준위 및 MLS/MCS범위에 대한 변환관계를 설정할수 있게 한다.(그림18)
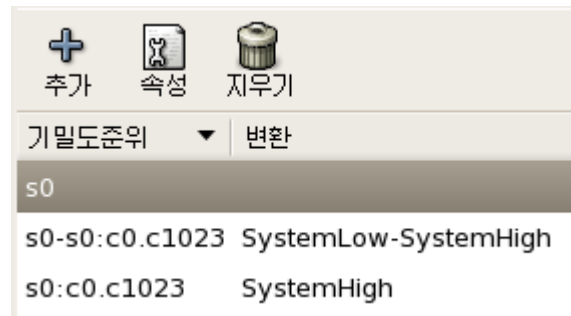
그림18. 변환관계 설정

기밀도준위를 추가하거나 변경, 삭제할수 있다.

기밀도준위에 대한 변환관계를 추가하거나 변경하는 경우에 기밀도준위값이 보안방책에 정의되여 있는 값이여야 한다.

- 망포구항목

이 항목은 망규약과 그 포구번호에 대한 보안문맥을 설정할수 있게 한다.(그림19)
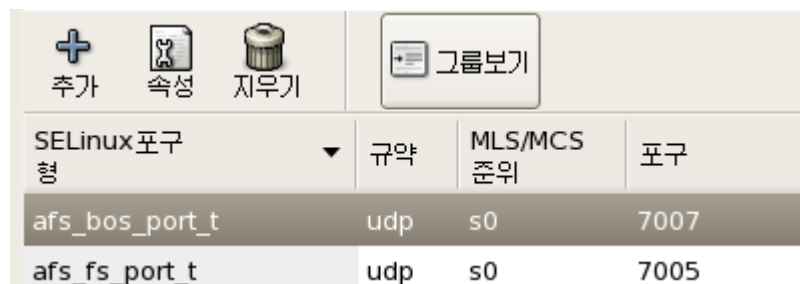
그림19. 망포구 설정

망포구에 대한 추가, 변경, 삭제가 가능하다. 추가나 변경시에 보안방책에 정의되여 있는 값들을 리용하여야 한다.

- 보안방책모듈

이 항목은 보안방책모듈을 추가하거나 삭제할수 있게 한다.(그림20)

그림20. 보안방책모듈 설정

다음으로 이 보안방책모듈들에 대하여 기록파일에 나타나지 않는 검사규칙들을 리용가능하게 하겠는가 리용불가능하게 하겠는가를 설정할수 있다. 모듈을 추가하는 경우 모듈파일은 /usr/share/selinux/targeted/안의 *.pp파일들이여야 한다. 그 이외의 파일들에 대하여서는 추가할수 없다. 그리고 base.pp와 enableaudit.pp는 기초모듈이므로 이 모듈들은 [추가]단추를 리용하여 적재할수 없다. 이 모듈들을 추가하는 경우 오유 통보문을 현시한다.

3.4 보안방책검사해석

이 기능은 주어진 체계기록파일로부터 보안리눅스관련 통보문들을 분석하고 통보문의 변경을 주어진 방책으로부터 추출한다.

도구의 주요기능은 다음과 같다.

1) 보안리눅스 검사통보문 열람과 정렬.
2) 보안리눅스 검사통보문 려과
3) 주어진 검사통보문으로부터 보안방책의 질문
4) 보안리눅스 검사통보문 파일에로의 출력
5) 전체 검사통보문에 대한 초본문 혹은 평문형식의 보고서 작성
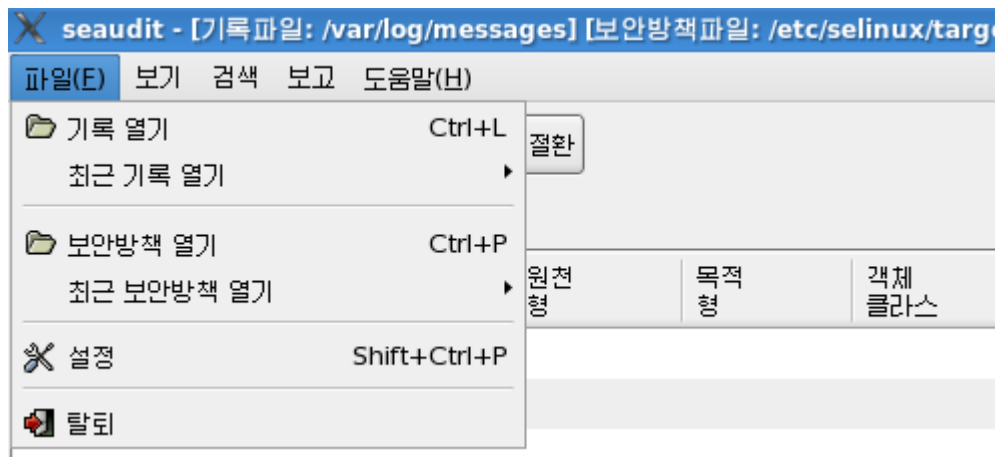
그림21. 보안방책검사해석도구

- 기록파일과 방책파일

도구는 기동시에 두개의 파일, 기록파일과 방책파일을 요구한다.(그림

21)

보안방책파일로서 2진 및 원천파일을 열수 있으며 기록파일로서 보안리눅스 검사통보문이 들어있는 모든 파일들을 열수 있다.

보안방책파일을 열지 않은 경우에는 일부 기능들을 사용할수 없게 된다.

기록파일을 열때 다음과 같은 경고문이 발생한다.

《경고:검사기록에서 하나 또는 그 이상의 무효한 통보문이 발견되였다.》 이 통보문은 보안리눅스 검사통보문중에서 표준통보문마당(실례를 들어 시간, 주콤퓨터이름, 호출형 등등)을 얻을수 없는 통보문이 있다는것을 나타낸다. 다음의 경우에도 이 경고통보문이 현시된다.

- ㅇ 통보문이 부정확한 시간정보를 가지고 있는 경우
- ㅇ AVC통보문이 허가권한을 포함하지 않는다.
- ㅇ AVC통보문이 《거부》 혹은 《허가》로 표식되지 않은 경우
- ㅇ 적재된 방책관련통보문이 정확한 형식을 가지고 있지 않는 경우
- ㅇ 론리형관련통보문이 론리형변수목록을 가지고 있지 않는 경우

- 안내

ㅇ 《파일》안내는 보안방책파일과 기록파일에 대한 열기기능을 제공하며 통보문표시창의 출력항목을 설정할수 있게 한다.

기록파일의 기정경로는 /var/log/messages으로 설정되여 있으며 보안방책파일은 우선 원천보안파일을 참조하고 그것이 없는 경우는 2진보안방책파일(/etc/selinux/targeted/policy/policy.21)을 참조한다.

《설정》을 선택하여 통보문표시창의 마당들을 설정할수 있다.

ㅇ 《보기》안내는 통보문표시창에 결과를 려과하여 보여주는 기능을 제공한다. 보기안내에서 《보기》->《새로운》을 선택하여 려과기능을 가진 규칙을 창조할수 있다.(아래의 《보기 수정》단추를 참고)

《보관》 과 《다른 이름으로 보관》안내는 현재 출력된 통보문에 대한 파일보기설정값을 보관할수 있게 하게 하며 《보기를 출력》 안내는 파일로 전체 통보문내용을 출력한다.

《선택된 통보문을 출력》 안내항목은 전체 보기 대신에 선택된 통보문만을 파일로 출력한다.

ㅇ《검색》안내는 사용자가 적재된 보안방책에 기초하여 통보문을 려과하거나 통보문과 관련된 보안방책들을 질문할수 있게 한다.

이상의 안내기능들을 통보문표시창에서 마우스 오른쪽단추누르기를 통하여 리용할수도 있다.

ㅇ 《보고》 안내는 보안리눅스관련 통보문으로부터 초본문표식언어나 평문으로 보고서파일을 생성할수 있게 하여 준다.

《보고 생성》창에서 《입력》마당은 보고작성 원천을 기록파일의 전체 통보문으로 하겠는가, 현재 표시창에 출력된 통보문으로 하겠는가를 설정할수 있게 한다. 《불완전한 통보문 포함》은 전체통보문을 선택하는 경우에만 유효하다.

다음으로 《출력》마당은 보고서파일에 대한 형식을 지정할수 있게 한다. 《일반본문》, " HTML" 로 설정할수 있는데 "HTML" 로 설정하는 경우 양식을 선택해야 한다. 기정양식은 /usr/share/setools/안에 보관되여 있다.

- 도구띠

ㅇ 《보안방책 질문》 단추

이 기능은 보안방책분석도구에서 형시행규칙검색과 류사한 검색항목을 설정할수 있게 한다.(그림22)

그림22. 보안방책질문대면부

원천형과 목적형, 객체클라스에 기초하여 형시행규칙을 검색한다. 이때 원천형과 목적형, 객체클라스는 현재 출력된 통보문에 표시된 형과 클라스들을 참고한다.

ㅇ 《보기 수정》 단추(려과기능 생성/편집)

이 기능은 표시되는 통보문들을 려과하여 보여줄수 있게 한다. 이 단추를 누르면 려과기능을 설정할수 있는 대화창이 현시된다. 이 대화창에서 새로운 려과기능의 추가 및 편집, 삭제, 파일로부터의 반입, 려과기능의 적용과 파일로의 보관을 진행할수 있다. 새로운 려과기능을 추가하려고 할때 새로운 대화창이 현시된다.(그림23)

보안문맥 기타 날자 주의

원천보안문맥

형:

사용자:

역할:

목적보안문맥

형:

사용자:

역할:

객체클라스

객체클라스:

그림23. 려과기 설정대면부

여기서는 보안문맥과 날자를 비롯한 기타 설정항목들을 설정할수 있게 한다.(편집시에도 같은 대화창이 현시된다.) 《보안문맥》표쪽은 원천보안문맥과 목적보안문맥, 객체클라스를 입력할수 있게 한다. 보안문맥의 매 항목인 형, 역할, 사용자, 객체클라스는 기록파일이나 적재된 보안방책파일로부터 값을 설정할수 있다.

《기타》표쪽은 망(IP주소, 포구대면부)과 관련된 려과기능을 설정할수 있게 한다.

이전에 생성한 려과기능을 편집하려면 려과기를 선택하고 《편집》단추를 누른다. 편집기능은 자동적으로 보관된다.

ㅇ 《감시절환》 단추

이 기능은 보안리눅스관련 통보문에 대한 실시간기록감시를 설정할수 있게 한다. 감시가 완료될때 상태띠에서 감시기상태표식이 《중지》로 된다. 이때 그 단어는 빨간색으로 표시된다. 이것이 기동할때 도구는 일정한 간격으로(기정적으로 초당) 새로운 통보문들에 대한 검사를 진행한다. 이 간격을 선택창으로부터 택할수 있다. 새로운 통보문을 발견하면 그것들은 표시창에 현시되게 된다.

3.5 보안방책비교

보안방책비교기능은 두개의 주어진 보안방책파일을 분석하고 차이점을 목록으로 보여줌으로써 그것들을 비교하는 기능이다.(그림24)
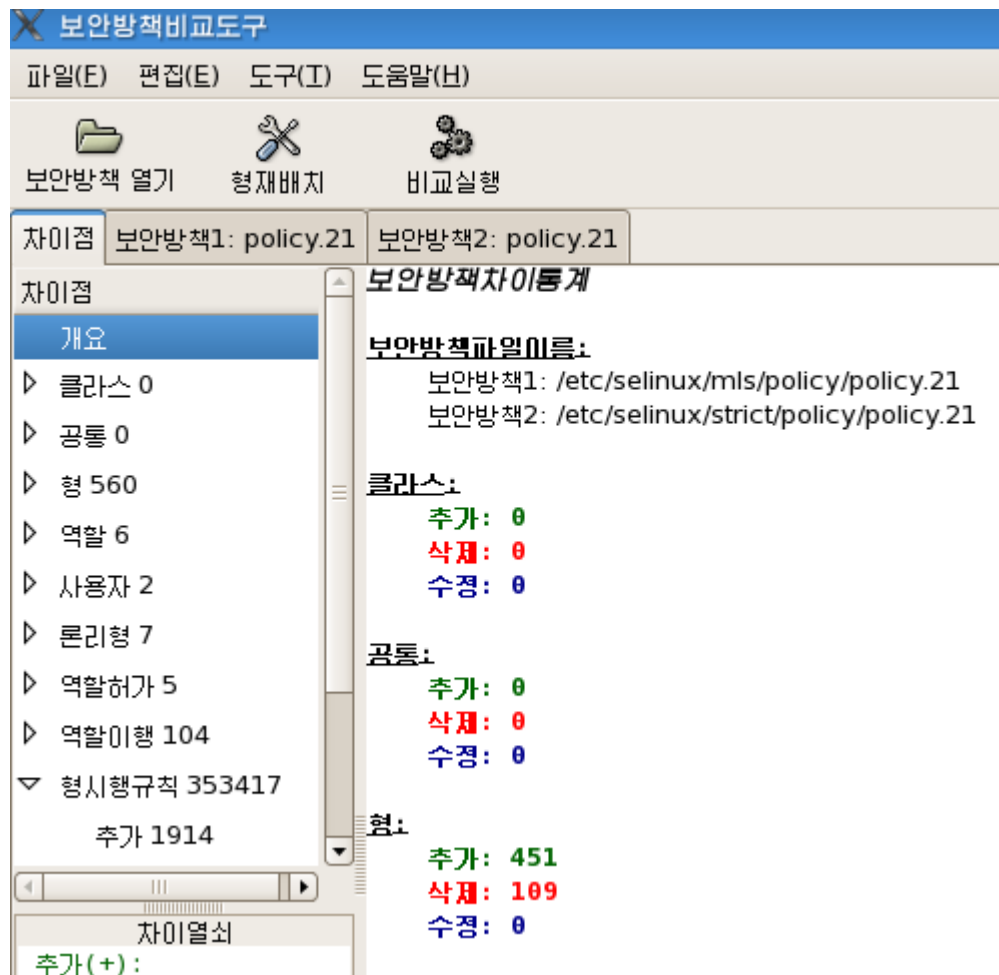
그림24. 보안방책비교도구

도구는 원천(판본12이상) 및 2진방책(판본15이상)을 비교할수 있으며 서로 다른 판본의 보안방책도 비교할수 있다.

보안방책비교도구는 현재 다음과 같은 방책 부분품들을 비교한다.

+객체 클라스와 허가속성들

+형과 속성들

+역할들

+사용자들

+론리형(booleans)
+형시행 규칙들(allow,type_transition 등등)
+역할허가 규칙들
보안방책비교도구의 기본기능은 매개 방책을 의미있게 분석하는것이다.
- 보안비교도구의 규칙:
왼쪽창문에서 보안방책 부분품별로 비교결과를 수값으로 보여준다. 부분품을 선택하면 오른쪽창문에 구체적인 비교결과들이 현시된다.
비교결과를 다음의 3개 형태로 보여준다.
+ 추가됨(+):방책 부분품이 방책 2에 의해서 추가되였다.
(방책 1이 아니라 방책 2에)
+ 삭제됨(-):방책 부분품이 방책 2에 의해서 삭제되였다.
(방책 2가 아니라 방책 1에)
+ 변경됨(*):방책 부분품이 두 방책에 다 표현되였다.
그러나 방책 2에 의해서 변경되였다.
ㅇ 클라스와 허가권한
이 부분품은은 방책의 3가지 측면을 검사한다. 클라스 정의, 공통허가권한 정의와 허가권한
ㅇ 클라스
클라스는 추가, 삭제, 변경될수 있다.
변경되였다는것은 클라스와 관련된 허가권한이 두 방책들 사이에 변경이 되였다는것을 의미한다.
ㅇ 공통허가권한
공통허가권한은 대체로 클라스와 같이 비교된다. 그것은 추가, 삭제, 변경될수 있는데 그것은 공통허가권한과 관련된 허가권한이 변화되였다는것을 의미한다.
ㅇ 허가권한
허가권한은 추가 혹은 삭제될수 있다. 그것들은변경될수 없다.
ㅇ 형
형은 추가, 삭제, 변경될수 있다. 변경은 형과 관련된 속성들이 두 방책들사이에 차이가 있다는것을 의미한다. 속성은 형으로부터 추가 및 삭제될수 있다.
ㅇ 속성
속성은 형과 같이 비교된다. 추가 및 삭제, 변경이 가능하다. 변경은 속성과 관련된 형이 차이가 있다는것을 의미한다.

(형은 속성으로부터 추가 혹은 삭제 될수 있다.)

ㅇ 역할

역할은 추가, 삭제, 변경될수 있다. 변경은 역할과 관련된 형이 두 방책들 사이에 차이가 있다는 것을 의미한다.

형은 역할로부터 추가 혹은 삭제될수 있다.

ㅇ 사용자

사용자는 추가, 삭제, 변경될수 있다. 변경되였다는것은 사용자와 관련된 역할이 두 방책들사이에 차이가 있다는것을 의미한다.

역할은 사용자로부터 추가 및 삭제될수 있다.

ㅇ 론리형

론리형은 추가, 삭제, 변경될수 있다. 만일 판본 15 혹은 초기 방책과 판본 16 혹은 그 이후 방책을 비교한다고 하자.

모든 론리형은 추가/삭제 되게 된다.(론리형은 판본 16에 들어있다.) 변경은 기정 값이 두 방책들사이에 차이가 있다는것을 의미한다.

ㅇ 형시행규칙

형시행규칙 령역은 방책의 《내용》들을 포함한다. 이 령역은 접근벡토르규칙들(allow, audit_allow, dont_audit)과 형관련규칙들(type_transition, type_change)을 포함한다. 모든 규칙들은 《원천-목적-클라스》(STC)에 기초하여 검색된다.

다음으로 조건규칙과 비조건규칙들을 구별하여 보여준다. 례를 들면 같은 STC를 가진 두개의 규칙들이 한개가 비조건규칙이고 다른 하나가 조건규칙인가 혹은 둘다 서로 다른 조건표현으로 규정되지 않은 조건규칙인가를 비교한다. 조건규칙은 그와 관련된 조건표현을 표시할뿐 아니라 《참》 혹은 《거짓》에 의해서 표시된다.

조건규칙에 대해서 론리형의 기정 및 현재 값은 무시된다. 조건표현은 론리형값은 모두 같다고 가정하고 비교된다.

규칙은 추가, 삭제, 변경될수 있다. 추가되였다는것은 방책 1에는 나타나지 않고 방책 2에는 있는 STC를 의미한다.

삭제되였다는것은 방책 1에는 있고 2에는 없는 STC를 의미한다. 접근벡토르규칙들에서 변경은 규칙에 대한 허가속성들이 그 방책들사이에 차이가 있다는것을 의미한다. 형규칙들에 대해서 변경은 기정형이 방책들사이에 차이가 있다는것을 의미한다.

ㅇ RBAC규칙

RBAC는 역할허가와 역할이행 규칙을 포함한다. 역할허가규칙들은 어떤 역할이 다른 역할로 이행이 허가되여 있는가를 결정한다.

첫번째 방책에 이 원천과 관련된 규칙이 없다면 그것이 추가된것이며 마찬가지로 두번째 방책에 규칙이 없다면 그것은 삭제된것이다.

만일 같은 원천을 가진 역할허가가 두 방책에 다 존재한다면 그 목적 역할은 변경으로서 보여준다.

- 방책표쪽:

이 표쪽은 매 방책에 대한 통계정보와 원천방책인 경우 원천파일의 내용을 현시한다.(그림25)

그림25. 방책표쪽

보안방책에 대한 통계정보로서 클라스와 허가권한개수, 형과 속성개수, 형시행규칙개수, 역할개수, RBAC규칙개수, 사용자수, 론리형개수를 보여준다.

- 형시행규칙정렬

형시행규칙에 대한 정렬은 《도구》안내의 《형시행규칙정렬》항목에 의해 진행된다.(그림26)
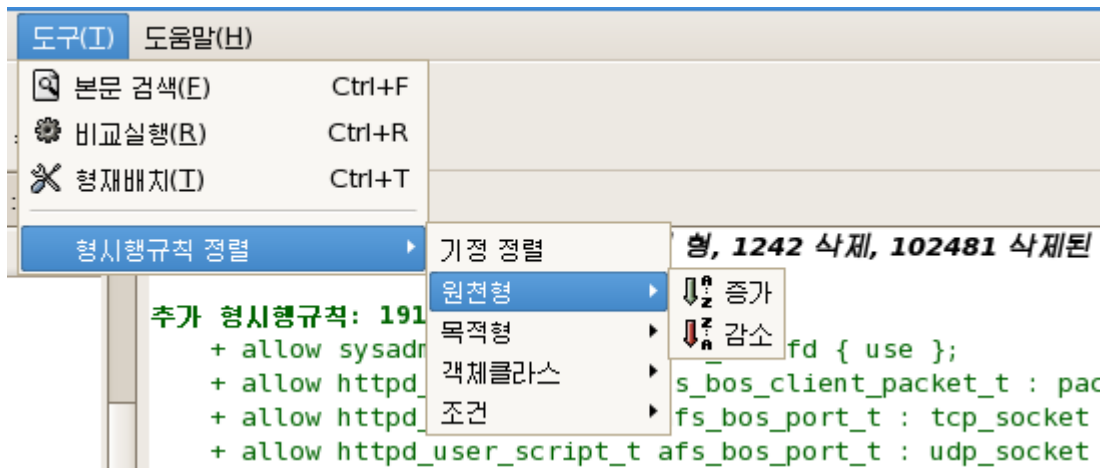
그림26. 형시행규칙정렬

도구는 다음과 같은 5가지 정렬방식을 지원한다.

《기정정렬》, 《원천형》정렬, 《목적형》정렬, 《객체클라스》정렬, 《조건》정렬이다. 기정정렬을 제외한 모든 정렬은 비교된 형시행규칙들에 관하여 영어자모순으로 규칙들을 정렬하여 보여준다.

이 안내는 형시행규칙을 선택한 경우에만 리용할수 있다.

4. 핵심부보안방책도구의 리용에서 알아야 할 점

4.1 주의점

- 도구를 기동하려면 현재 체계가 [시행방식]이나 [허가방식]으로 동작하여야 한다.
- 보안설정도구를 기동하려면 /etc/selinux/*/안에 setrans.conf파일이 있어야 한다. 이 파일은 MLS/MCS준위 및 범위에 대한 변환관계를 정의하고 있다. *는 보안방책의 형을 나타낸다. 즉 "strict"인가, " targeted"일수 있다.

4.2 제기되는 문제

보안방책개발도구를 리용하면서 제기되는 문제들에 대해서는 다음의 전화번호로 전화하여 주십시오.

전화번호: 358-2467

5. 주해